MAT0265 Grupos

Lista 1

Exercícios 10 e 25

Pedro Gigeck Freire

10737136

(10) Seja G um grupo e seja H um subconjunto não vazio finito de G tal que $HH = H$. (Sendo $HH = \{ab : a, b \in H\}$). Prove que H é um subgrupo de G. E se H não for finito?

Seja $e \in G$ o elemento neutro de G.

- Vamos mostrar que $e \in H$.

Como $H \neq \emptyset$, existe $a \in H$.

Seja $a \in H$, vamos provar que a^i, com $i \in \{1, 2, \cdots\}$, $\in H$.

Prova por indução em i:

- Base: $(i = 1)$

  $a^1 = a \in H$.

- Suponha que para $i \leqslant n$, $a^i \in H$.

  Como $a, a^n \in H$, então $aa^n \in HH$.

  Mas $HH = H$, então $aa^n = a^{n+1} \in H$.

O resultado segue pelo princípio da indução.

Então $\{a^i : i \in \{1, 2, 3, \dots\}\} \subseteq H$.

Como H é finito, existem $i, j \in \{1, 2, \dots\}$ tais que $a^i = a^j$, pois se não existisse todos os $a^i \in H$ seriam diferentes então H seria infinito.

Podemos supor, sem perda de generalidade, que $j > i$, logo

$$a^j = a^i \Rightarrow a^j a^{-i} = a^i a^{-i} \Rightarrow a^{j-i} = e.$$

Como $a^{j-i} \in H$, $e \in H$.

• Se $a,b \in H$, então $ab \in HH$, mas $HH = H$, então $ab \in H$.

• Seja $a \in H$, vimos que existem $i, j \in \{1, 2, \dots\}$ tais que $a^{j-i} = e$, com $j > i$

Se $j-i = 1$, então $a = e$.

Se $j - i > 1$, então $a\, a^{j-i-1} = e \Rightarrow a^{j-i-1}$ é o inverso de a;

como $j-i-1 > 0$, então $a^{j-i-1} = a^{-1} \in H$.

Portanto, $e \in H$; $a,b \in H \Rightarrow ab \in H$; $a \in H \Rightarrow a^{-1} \in H$.

Então H é subgrupo de G.

Se H é infinito, o resultado não vale. Por exemplo:

$G = (\mathbb{Z}, +)$

$H = \{0, 1, 2, \dots\} = \{i \in \mathbb{Z} : i \geq 0\} \subseteq G$.

• Seja $a \in H$, então $a = 0 + a \Rightarrow a \in HH \Rightarrow H \subseteq HH$

• Seja $a \in HH$, com $a = b + c$, temos que $a \geq 0 \Rightarrow a \in H \Rightarrow HH \subseteq H$.

Logo, $H = HH$.

Mas H não é subgrupo, pois há elementos sem inverso aditivo em H.

(Ou seja, $a \in H \Rightarrow a = 0$ ou $\nexists\, (-a) \in H$ tq $a + (-a) = 0$).

(25) Mostre que o número de geradores de um grupo cíclico de ordem n é $\varphi(n)$, onde $\varphi(n)$ é a função de Euler ($\varphi(n)$ é igual ao número de inteiros positivos menores que n e que são relativamente primos com n).

Vamos precisar de alguns resultados intermediários.

Seja G um grupo cíclico de ordem n.

(i) (Exercício 16) Se $a \in G$ tem ordem finita n, então $|\langle a \rangle| = n$.

Seja $D = \{0, 1, \dots, n-1\}$

Seja $f : D \longrightarrow \langle a \rangle$ dada por $f(i) = a^i$

Vamos mostrar que f é uma bijeção

(sobrejeção) Seja $x \in \langle a \rangle$, então existe $i \in \mathbb{Z}$ tal que $x = a^i$.

Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$, com $0 \leq r < n$ tais que $i = qn + r$.

Logo $x = a^i = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r = e^q a^r = e a^r = a^r$.

Mas $r \in D$, então $x = a^i = a^r = f(r) \in f(D)$.

Portanto $\langle a \rangle \subseteq f(D) \Rightarrow f$ é sobrejetora.

(injeção) Seja $i, j \in D$ tais que $f(i) = f(j)$

Suponha, por absurdo, que $i \neq j$

- Se $j > i$, então $a^i = a^j \Rightarrow a^{j-i} = e$

Mas n é o menor inteiro positivo tal que $a^n = e$, logo

$j - i > n \Rightarrow j > n + i > n \Rightarrow j \notin D$, absurdo.

- Se $i > j$, analogamente, $a^{i-j} = e \Rightarrow i - j > n \Rightarrow i > n \Rightarrow i \notin D$, absurdo

Por contradição, $j = i$, então f é injetora.

Portanto f é bijetora, então $|\langle a \rangle| = |D| = n$.

(ii) $a \in G$ gerador de $G \iff a$ tem ordem n.

($\Rightarrow$) a gerador de $G \Rightarrow \langle a \rangle = G \Rightarrow |\langle a \rangle| = |G| = n$

Suponha que a tenha ordem finita $m \neq n$.

Por (i), $|\langle a \rangle| = m$, contradição.

Como G é finito, a ordem de a é finita e igual a n.

($\Leftarrow$) a tem ordem n, então, por (i) $|\langle a \rangle| = n = |G|$, como $\langle a \rangle \subseteq G$ então $\langle a \rangle = G$. Portanto a é gerador.

(iii) (Exercício 21) Seja $a \in G$ tal que $a^n = e$, então ordem de a divide n.

Seja m a ordem de a

Temos que $n \geq m$

Se $n = m$, então m divide n.

Se $n > m$, pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$, $0 \leq r < m$ tais que

$n = qm + r$, então $a^n = a^{qm+r} = a^{qm} a^r = e a^r = a^r$, mas $r < m$,

então $r = 0$.

Portanto $n = qm \Rightarrow m$ divide n.

(iv) (Exercício 24) Se $a \in G$ tem ordem n, seja i um inteiro positivo tal que $mdc(i, n) = 1$, então a^i tem ordem n.

$a^n = e \Rightarrow (a^n)^i = e^i \Rightarrow (a^i)^n = e^i = e$.

Seja n' a ordem de a^i.

Então $a^n = (a^i)^{n'} = a^{in'}$, por (iii) $n \mid in'$, logo, existe $q \in \mathbb{Z}$ tq

$$in' = qn \Rightarrow i = \frac{qn}{n'}.$$

Como $(a^i)^n = e$, então $n' \mid n$, logo existe $q' \in \mathbb{Z}$ tal que

$$n = q'n' \Rightarrow \frac{n}{n'} = q'$$

Então

$$i = \frac{qn}{n'} = qq' \Rightarrow q' \mid i,$$ mas q' divide n, pois $n = n'q'$.

Portanto

$$mdc(i, n) = q' \Rightarrow q' = 1 \Rightarrow n = n'q' = n'.$$

(v) Se $a \in G$ tem ordem n, seja i um inteiro positivo tal que $mdc(i,n) = d$, com $d > 1$, então a^i tem ordem menor que n.

$mdc(i,n) = d \Rightarrow n = qd$ e $i = q'd$ para $q, q' \in \mathbb{Z}$.

Logo $e = a^n = a^{qd} \Rightarrow e^{q'} = (a^{qd})^{q'} = a^{qdq'} = (a^{q'd})^q = (a^i)^q$

Mas sabemos que $0 < q < n$, então a^i tem ordem menor que n.

Portanto, de (ii) sabemos que

$a \in G$ gerador $\Leftrightarrow$ a tem ordem n.

Seja $a \in G$ gerador, sabemos que $\langle a \rangle = G = \{a^1, a^2, a^3, \dots, a^n\}$

De (iv) e (v) sabemos que

a^i tem ordem $n \Leftrightarrow mdc(i,n) = 1$

Logo, $x = a^i \in \langle a \rangle$ é gerador $\Leftrightarrow mdc(i,n) = 1$.

Seja $X = \{x \in G : x$ é gerador de $G\}$

Então $X = \{a^i \in \langle a \rangle : i \in \mathbb{Z}^+$ e $mdc(i,n) = 1\}$

Por definição $|X| = \varphi(n)$.

∎